日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: １９９９年１２月２０日

出願番号
Application Number: 平成１１年特許願第３６１２２１号

出願人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ８月 ４日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６２４５９

【書類名】　特許願

【整理番号】　9900272402

【提出日】　平成11年12月20日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　1/00　410

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　渡辺　一夫

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ソフトウエア使用制御方法とその装置

【特許請求の範囲】

【請求項１】

ソフトウエア提供者側は、提供対象のソフトウエアと、該ソフトウエアに対応して用意されて該ソフトウエアを稼働する装置に接続する部材であって、前記接続された状態で該装置よりアクセス可能であり、内部に、前記対応するソフトウエアごとの所定の第１の情報が記憶されている部材とが配付されたソフトウエア使用者側に対して、前記部材に記憶されている前記第１の情報と照合する第２の情報を、公開鍵暗号方式の秘密鍵を用いて暗号化し、

前記暗号化した前記第２の情報を、前記ソフトウエア使用者側に送信し、

前記ソフトウエア使用者側は、前記伝達された暗号化された前記第２の情報を、前記公開鍵暗号方式の公開鍵を用いて復号し、

前記部材より前記第１の情報を読み出し、

前記読み出した前記第１の情報と前記復号した前記第２の情報とを照合し、

該照合が一致した場合に前記ソフトウエアの使用を可能とする

ソフトウエア使用制御方法。

【請求項２】

前記ソフトウエア使用者側は、前記ソフトウエアの使用の許諾を求める際に、前記提供対象のソフトウエアおよび前記部材とともに配付される前記ソフトウエアを特定する所定の第３の情報を、前記ソフトウエア使用者側に伝達し、

前記ソフトウエア提供者側は、前記伝達された前記第３の情報に基づいて、前記ソフトウエア使用者側を特定し、該ソフトウエア使用者側に配付されている前記部材に記憶されている前記第１の情報と照合する前記第２の情報を検出し、

該第２の情報を前記暗号化する

請求項１に記載のソフトウエア使用制御方法。

【請求項３】

前記第１の情報および前記第２の情報は、前記ソフトウエア使用者を特定する識別情報、または、前記配付されたソフトウエアまたは部材を特定する識別情報

出証特２０００－３０６２４５９

であり、

前記第２の情報は、前記ソフトウエアおよび前記部材に添付されたパスワードである

請求項２に記載のソフトウエア使用制御方法。

【請求項４】

前記ソフトウエアの使用を制御する処理を、前記ソフトウエア使用者側において前記ソフトウエアの使用を行なう都度行なう

請求項３に記載のソフトウエア使用制御方法。

【請求項５】

前記ソフトウエアの使用を制御する処理を、ソフトウエア入手時、ソフトウエアのバージョンアップ時またはソフトウエアの利用期限の設定、更新時のいずれかを含む、予め定めた所定の時にのみ行なう

請求項３に記載のソフトウエア使用制御方法。

【請求項６】

配付された使用対象のソフトウエアを記憶する記憶手段と、

所定のインターフェイス手段を介してアクセス可能に接続された部材であって、前記記憶しているソフトウエアごとの所定の第１の情報が記憶されている部材と、

前記記憶しているソフトウエアの使用の許諾を求める際に、当該ソフトウエアを特定する第３の情報を、ソフトウエア提供者側に送信する送信手段と、

前記ソフトウエア提供者側より伝送される、前記第３の情報に基づいて生成された前記第１の情報と照合する第２の情報を公開鍵暗号方式の秘密鍵を用いて暗号化された情報を受信する受信手段と、

前記受信した暗号化された第２の情報を、前記公開鍵暗号方式の公開鍵を用いて復号する復号手段と、

前記部材に記憶されている前記第１の情報と前記復号した前記第２の情報とを照合する照合手段と、

該照合が成功した場合に前記ソフトウエアを使用可能とする実行制御手段とを有するソフトウエア使用制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、たとえばコンピュータプログラムなどのソフトウエアの不正利用を防止し、適正な使用者のみ使用可能にするソフトウエア使用制御方法とその装置に関する。

【０００２】

【従来の技術】

たとえばコンピュータプログラムなどのソフトウエアを頒布する際には、ソフトウエアの不正コピーや不正偽造を防止し、使用を許諾した適正な使用者にのみ使用を可能な状態で頒布することが重要である。

従来、このような不正利用対策としては、パスワードを利用する方法や、ドングルやＩＣカードなどを利用する方法がとられている。

前者は、ソフトウェアの起動時に各ソフトウェアごとのパスワードを入力しなければソフトウエアが有効に動作しないようにしたもので、ソフトウェア内で入力されたパスワードと予め登録されているパスワードとの照合を行なうことにより実現される。なお、このパスワードとしては、秘密鍵などが用いられている場合が多い。

【０００３】

後者は、ドングルやＩＣカードをソフトウエアとともに配付し、ソフトウエア起動時に、各ソフトウエアの識別子と、ドングルやＩＣカードに記述されている識別子との照合を行なうものである。この識別子も、通常、秘密鍵などが用いられている。この方法においては、ソフトウエア内の秘密情報が解読されても、ドングルやＩＣカードがなければソフトウエアを利用することはできず、より安全性の高い方法と言うことができる。

【０００４】

【発明が解決しようとする課題】

しかしながら、前述したパスワードを用いる方法では、本来は漏洩しなように管理されている筈のパスワード（秘密鍵）自体が、意図的に、あるいは、偶発的

に適正な利用者以外の者に伝わり、ソフトウエアが不正利用されてしまう可能性があり、また、実際にそのような不正利用も多く発生している。

また、ドングルやＩＣカードを用いる方法においても、そのドングルやＩＣカードの偽造や複製が完全に不可能であるとは言い切れず、偽造や複製されソフトウエアが不正利用される可能性がある。また、この方法では、ソフトウエアのバージョンアップや変更などに合わせて、ドングルやＩＣカードを再配付しなければならず、処理が面倒である上に、コストもかかるという問題がある。

【０００５】

したがって、本発明の目的は、より高い安全性でソフトウエアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウエア使用制御方法を提供することにある。

また、本発明の他の目的は、より高い安全性でソフトウエアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウエア使用制御装置を提供することにある。

【０００６】

【課題を解決するための手段】

前記課題を解決するために、本発明のソフトウエア使用制御方法においては、ソフトウエア提供者側は、提供対象のソフトウエアと、該ソフトウエアに対応して用意されて該ソフトウエアを稼働する装置に接続する部材であって、前記接続された状態で該装置よりアクセス可能であり、内部に、前記対応するソフトウエアごとの所定の第１の情報が記憶されている部材とが配付されたソフトウエア使用者側に対して、前記部材に記憶されている前記第１の情報と照合する第２の情報を、公開鍵暗号方式の秘密鍵を用いて暗号化し、前記暗号化した前記第２の情報を、前記ソフトウエア使用者側に送信し、前記ソフトウエア使用者側は、前記伝達された暗号化された前記第２の情報を、前記公開鍵暗号方式の公開鍵を用いて復号し、前記部材より前記第１の情報を読み出し、前記読み出した前記第１の情報と前記復号した前記第２の情報とを照合し、該照合が一致した場合に前記ソフトウエアの使用を可能とする。

【０００７】

また、本発明のソフトウエア使用制御方法は、配付された使用対象のソフトウエアを記憶する記憶手段と、所定のインターフェイス手段を介してアクセス可能に接続された部材であって、前記記憶しているソフトウエアごとの所定の第１の情報が記憶されている部材と、前記記憶しているソフトウエアの使用の許諾を求める際に、当該ソフトウエアを特定する第３の情報を、ソフトウエア提供者側に送信する送信手段と、前記ソフトウエア提供者側より伝送される、前記第３の情報に基づいて生成された前記第１の情報と照合する第２の情報を公開鍵暗号方式の秘密鍵を用いて暗号化された情報を受信する受信手段と、前記受信した暗号化された第２の情報を、前記公開鍵暗号方式の公開鍵を用いて復号する復号手段と、前記部材に記憶されている前記第１の情報と前記復号した前記第２の情報とを照合する照合手段と、該照合が成功した場合に前記ソフトウエアを使用可能とする実行制御手段とを有する。

【０００８】

【発明の実施の形態】

本発明の一実施の形態について、図１～図６を参照して説明する。

本実施の形態においては、ソフトウエア販売会社が利用者にソフトウエアを販売し、利用者がそのソフトウエアを実際に使用する手順を説明することにより、本発明を説明する。

【０００９】

まず、ソフトウエア販売会社が利用者にソフトウエアを販売する際の処理について、図１を参照して説明する。

まず、販売会社１０は、ソフトウエアに、商品番号、ラベル名などそのソフトウエアを特定することのできるパスワード１１を添付し、また、ドングルに、製品番号、ドングル番号、有効期日（恒久的に使用権限があるのか、利用期限付での使用権限か）など、ソフトウエアの使用形態に応じて決まる特定の識別情報１２を内包させ、利用者２０に配付する。

この時、販売会社１０は、パスワード１１と識別情報１２および配付した利用者２０との対応を管理しておく。特に、識別情報１２に関しては、秘密の状態で

管理しておく。

【００１０】

次に、販売会社１０は、販売会社のみに秘密にしておく公開鍵暗号方式による秘密鍵１３と、それに対応する利用者用の公開鍵１４を作成する。

そして、販売会社１０は、各利用者に、利用者用の公開鍵１４を伝達する。

販売会社が作成するこの秘密鍵１３および公開鍵１４の対は、各利用者ごとに共通としてもよいし、別のものを用意してもよい。共通にすれば、管理が容易となり、また、別にすれば、安全性が高まる。

また、この際に用いる公開鍵および秘密鍵は、十分に安全とされているデジタル署名方式の枠組みを使用する。

【００１１】

次に、このような事前処理が終了した後に、使用者が実際に使用許諾を得て、ソフトウエアを使用する処理について、図２を参照して説明する。

まず、利用者２０は、ライセンスを得ようとした場合、ソフトウエアに添付されているパスワードを、販売会社に送信する（２１）。

販売会社は、利用者から受信したパスワードに基づいて、自ら管理している情報を検索して、各利用者ごとのソフトウエアの識別情報を検出する（２２）。

次に、販売会社は、検出した識別情報を、販売会社の秘密鍵を用いて暗号化し、暗号化ライセンス情報を生成する（２３）。

そして販売会社は、生成した暗号化ライセンス情報を、各利用者に送信する。（２４）。

【００１２】

利用者は、この暗号化ライセンス情報を受信したら、ソフトウエアを起動し、ソフトウエア内の処理により、受信した暗号化ライセンス情報とドングルに内包している識別情報との照合を行なう（２５）。

ソフトウエア内においては、まず、送信された暗号化ライセンス情報が公開鍵により復号され、利用者ごとのパスワードに対応したデータが得られる。

次に、ドングルに内包してある識別情報と照合される。

そして、照合に合格すれば、ソフトウエアは有効に起動されて所望の処理を行

ない（２６）、照合に失敗すればソフトウエアの実行を停止する（２７）。

【００１３】

このように、本実施の形態においては、ドングルに内包されている識別情報を用いてライセンスを行なっており、このようなドングルは、通常であれば利用者も知ることができないものである。したがって、ソフトウエアの使用を所望の形態に制御することができる。

また、ソフトウエアに受け渡す識別情報は、暗号化された形態となっており、この暗号化ライセンス情報を作成できるのは、秘密鍵を保持しているも販売会社のみである。したがって、仮に、識別情報を知り得たとしても、暗号化ライセンス情報を作成することは困難であり、よりセキュリティ高く、ソフトウエアの使用のライセンシーを制御できる。

【００１４】

次に、前述した実施の形態のより具体的な例について説明する。

なお、以下の説明において、ＰＮは購入時のソフトウエアに添付されている商品番号、ＤＩＤはドングルＩＤ番号、ＰＩＤはプロダクトＩＤ番号、ＣＫはセンター秘密鍵、ＵＫユーザー公開鍵、ｈは一方向性ハッシュ函数、（Ｒ，Ｌ）は暗号化ライセンス情報である。

なお、ここでは、Ｓｃｈｎｏｏｒ署名を用いた場合について説明する。

【００１５】

まず、販売会社での事前処理について、図３を参照して説明する。

まず、３２ビット程度の素数ｑを選び、次に、素数ｑがｐ－１の素因数となるような大きな１０２４ビット程度の素数ｐを選び、得られた素数ｐ，ｑを、ソフトウエアおよびドングルに記録しておく（３１）。

【００１６】

この素数ｑ，ｐの選び方について、図４を参照して説明する。

まず、選択処理を開始したら（ステップＳ１０）、たとえばラビン法などの確率的素数判定法を用いて３２ビット程度の素数ｑを選ぶ（ステップＳ１１）。

次に、同じく確率的素数判定法により３２０ビット程度の素数ｑ＿０を選ぶ（ステップＳ１２）。

次に、ｎ＝１とおき（ステップＳ１３）、同じく確率的素数判定法を用いてさらに素数ｑ＿ｎを選ぶ（ステップＳ１４）。

そして、ａ＝２×ｑ＿０×…×ｑ＿ｎを計算し（ステップＳ１５）、その計算結果ａのサイズが１０００ビット程度の所定のビット幅に達しているか否かをチェックする（ステップＳ１６）。

【００１７】

ａが１０００ビットに足らない場合には（ステップＳ１６）、ｎを１カウントアップして（ステップＳ１７）、ステップＳ１４以下の処理に戻る。すなわち、さらに次の素数ｑ＿ｎを選び（ステップＳ１４）、ａ＝２×ｑ＿０×…×ｑ＿ｎを計算し（ステップＳ１５）、結果ａのサイズが所定のビット幅に達しているか否かをチェックする（ステップＳ１６）。

このような処理を繰り返し、ステップＳ１６において結果ａのサイズが１０００ビット程度の所定のビット幅に達した場合には、ｐ＝ｑ×２×ｑ＿０×…×ｑ＿ｎ＋１を計算し（ステップＳ１８）、得られた値ｐが素数であるか否かを確定的素数判定法により判定する（ステップＳ１９）。

得られた値ｐが素数で無い場合には、ステップＳ１２に戻り、値ｐを得るためのステップＳ１２～ステップＳ１８の処理を繰り返す。

ステップＳ１９において、得られた価ｐが素数であれば、処理を終了する（ステップＳ２０）。

【００１８】

次に、法ｐに関する原始根ｇを選び、ｈ＝ｇ＾｛ｐ－１／ｑ｝mod ｐを計算し、これもソフトウエアおよびドングルに記録しておく（３２）。

この原始根ｇを選ぶ処理について、図５を参照して説明する。

なお、ｐ－１＝ｒ＿１×・・・×ｒ＿ｎとする。

まず、処理を開始したら（ステップＳ３０）、１＜ｇ＜ｐとなるｇをランダムに選ぶ（ステップＳ３１）。

次に、ｉ＝１とおいて（ステップＳ３２）、ａ＝ｇ＾｛ｐ－１／ｒ＿ｉ｝を計算し（ステップＳ３３）、計算結果ａがａ≠１mod ｐであるか否かをチェックする（ステップＳ３４）。

【００１９】

その結果、ａ＝１ｍｏｄ ｐの場合は、ステップＳ３１に戻り、再びｇを選択する処理から開始する。

ステップＳ３４において、ａ≠１ｍｏｄ ｐだった場合には、全てのｒ＿ｉに対してチェックを行なったか、すなわちｉ＝ｎか否かをチェックし（ステップＳ３５）、ｉ≠ｎの時には、ｉをカウントアップし（ステップＳ３６）、ステップＳ３３に戻り、次のｒ＿ｉのチェックを行なう。

そして、全てのｒ＿ｉに対してチェックを行なったら、その時に得られているｇを原始根として、処理を終了する（ステップＳ３７）。

【００２０】

次に、０＜ＣＫ＜ｑとなるように、販売会社の秘密鍵ＣＫを任意に選ぶ（３３）。この秘密鍵ＣＫは、販売会社だけの秘密として厳重に保管しておく。

【００２１】

次に、利用者の鍵ＵＫを式１に基づいて計算し、この鍵ＵＫを利用者に知らせておく（３４）。この利用者公開鍵ＵＫは、ソフトウエアの新規購入の時や、バージョンアプの時ごとに生成し、連絡する。

【００２２】

【数１】

$$UK = h^{\{p-1-CK\}} \bmod p \qquad \cdots (1)$$

【００２３】

次に、ソフトウエアに付属するドングルにソフトウエアの商品番号ＰＮ（３５）、これに対応するドングルＩＤ番号ＤＩＤ、および、プロダクトＩＤ番号ＰＩＤ（３６）を記録しておくとともに、これらを販売会社だけの秘密として厳重に保管しておく。

【００２４】

そして、一方向性ハッシュ函数Ｈ（１＜＝Ｈの値域＜＝ｑ）を用意し、これをソフトウエアおよびドングルに記録しておく（３７）。

以上が、販売会社１０で行なう事前処理の具体的内容である。

【００２５】

次に、実際にライセンスを管理し、利用者側におけるソフトウエアの実行を制御する方法について、図６を参照して具体的に説明する。

まず、利用者は、ソフトウエアを購入した時、あるいは、利用期限を更新する時などに、商品番号ＰＮを販売会社に送信する（６１）。

販売会社は、利用者より送信された商品番号ＰＮに基づいて、利用者のソフトウエアのＤＩＤおよびＰＩＤを獲得する（６２）。

次に、販売会社は、乱数ｋ（１＜ｋ＜ｑ）を生成し、式２に従って暗号化ライセンス情報（Ｒ，Ｌ）を生成し、利用者に送信する（６３）。

【００２６】

【数２】

$$R=H(DID,\ PID,\ h^{k} \bmod p) \quad 0<R<q \qquad \cdots (2)$$

$$L=CK\times R+k \bmod q$$

【００２７】

利用者は、受信した暗号化ライセンス情報（Ｒ，Ｌ）と商品番号ＰＮを用いて、また、ドングルから商品番号ＰＮに対応するＤＩＤ，ＰＩＤを読み込み、式３に示すような照合を行なう（６４）。

【００２８】

【数３】

$$H(DID,\ PID,\ H^{L}\times UK^{R} \bmod p)=R \qquad \cdots (3)$$

【００２９】

そして、式（３）が成立すれば、正当なユーザーであることを確認し、プログラムを有効に動作させ（６５）、不成立の場合は、プログラムを停止させる（６

６）。

このような具体的な処理により、前述した本実施の形態が実施できる。

【００３０】

なお、本発明は本実施の形態に限られるものではなく、種々の改変が可能である。

たとえば、本実施の形態においては、コンピュータプログラムを頒布する場合におけるライセンス管理方法を例示して本発明を説明したが、いわゆるライブラリと言われるような任意のシステムにおけるデータ、機能的な構造を有するデータなど、プログラム以外の種々のデータの使用に対しても適用可能である。

また、コンピュータ以外の任意の機械、システムなどで使用される、それらプログラムやデータなどについても適用可能である。

【００３１】

また、前述した具体例においては、Ｓｃｈｎｏｏｒ署名を用いる例を示したが、ＲＳＡ署名、ＤＳＡ署名、ＥｌＧｍａｌ署名、Ｆｉａｔ－Ｓｈａｍｉｒ署名、楕円曲線に基づく署名など、任意のデジタル署名方式を用いることができる。

また、本実施の形態においては、ソフトウエアとともにドングルを配付する例を示したが、ＩＣカードなどでもよい。

【００３２】

なお、前述した例においては、販売会社１０、利用者２０などの言葉を用いたが、実際に前述した処理が行なわれるのは、販売会社側の情報処理装置、利用者側の情報処理装置である。

【００３３】

【発明の効果】

このように、本発明によれば、より高い安全性でソフトウエアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウエア使用制御方法を提供することができる。

まが、より高い安全性でソフトウエアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウエア使用制御装置を提供することができる。

【図面の簡単な説明】

【図１】

図１は、本発明の一実施の形態のプログラム配信システムの配信事前処理を説明するための図である。

【図２】

図２は、本発明の一実施の形態のプログラム配信システムの処理を説明するための図である。

【図３】

図３は、本発明の一実施の形態のより具体的な例のプログラム配信システムの配信事前処理を説明するための図である。

【図４】

図４は、図３に示した処理において、素数ｐを求める処理を説明するためのフローチャートである。

【図５】

図５は、図３に示した処理において、原始根ｇを求める処理を説明するためのフローチャートである。

【図６】

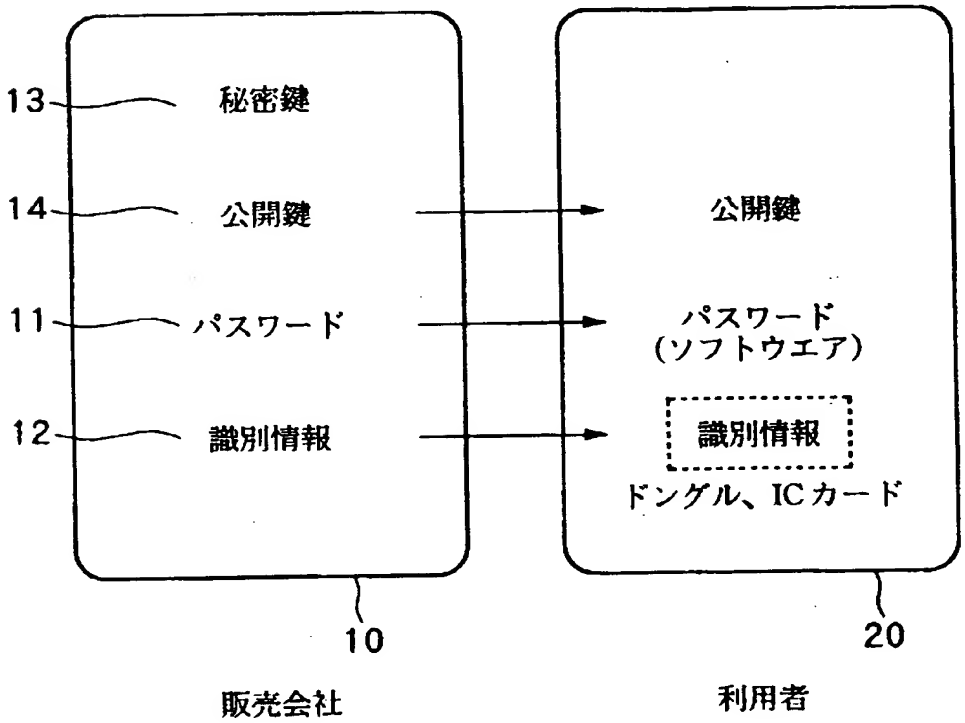
図６は、本発明の一実施の形態のより具体的な例のプログラム配信システムの処理を説明するための図である。

【符号の説明】

１０…販売会社、１１…パスワード、１２…識別情報、１３…秘密鍵、１４…公開鍵、２０…利用者

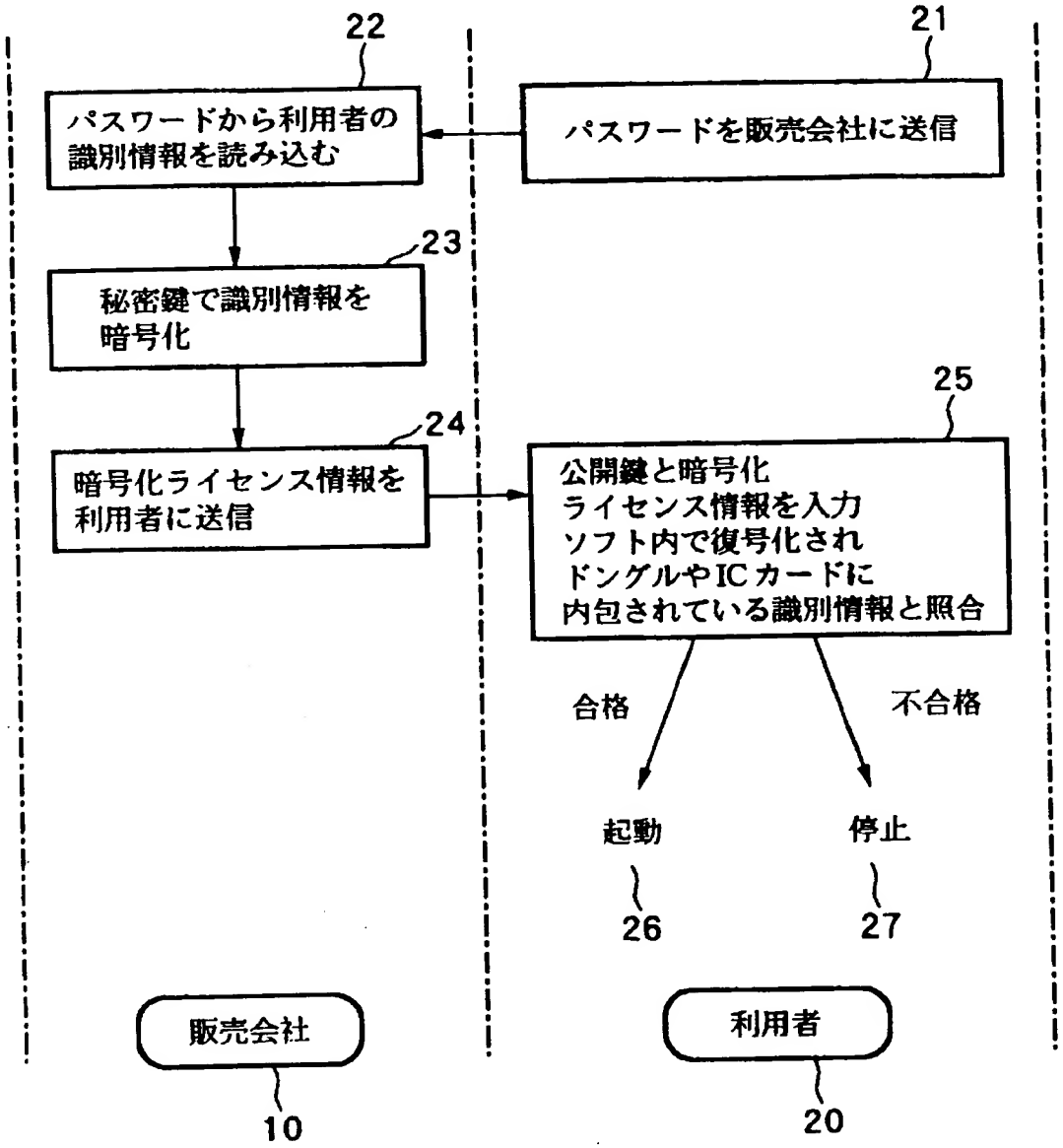
【書類名】　図面

【図１】



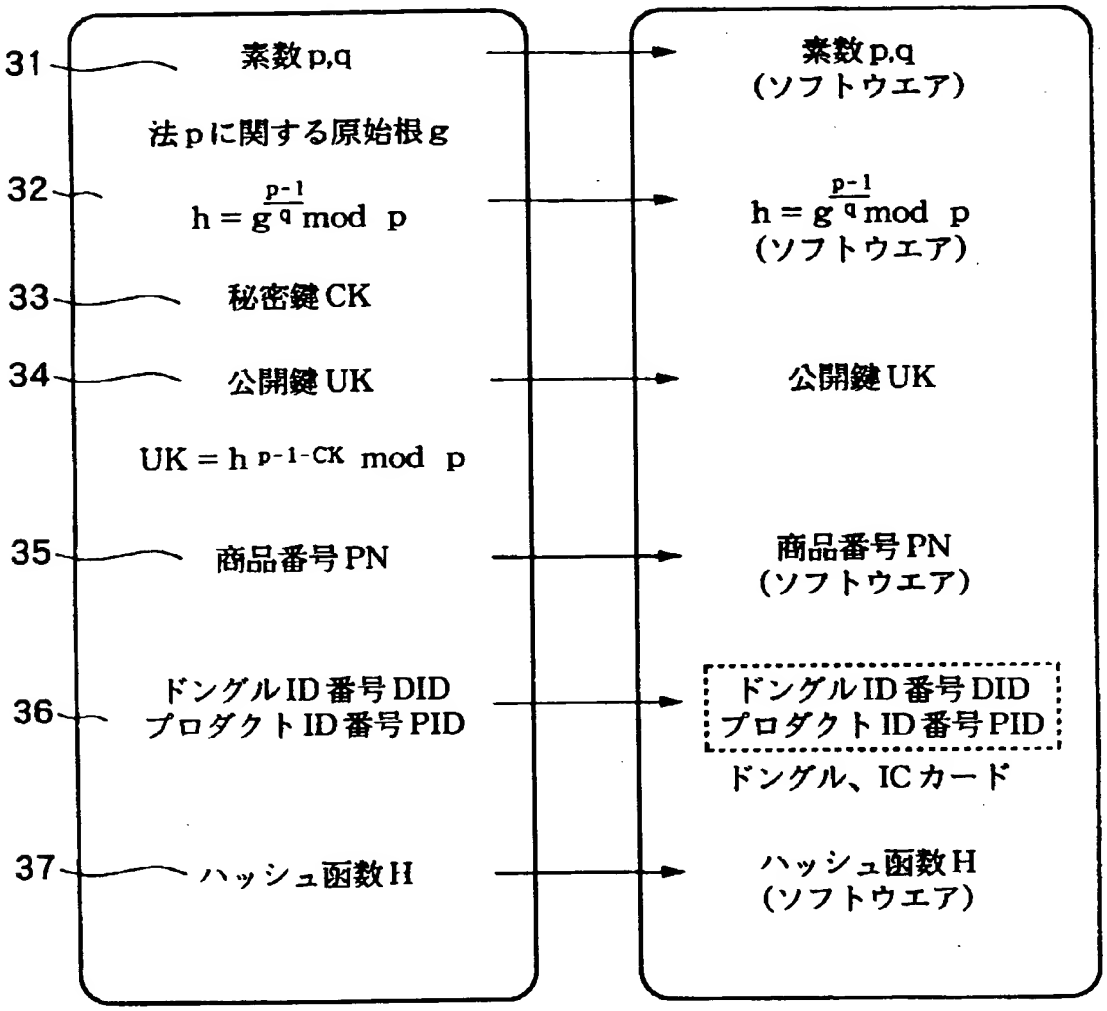
出証特２０００－３０６２４５９

【図２】

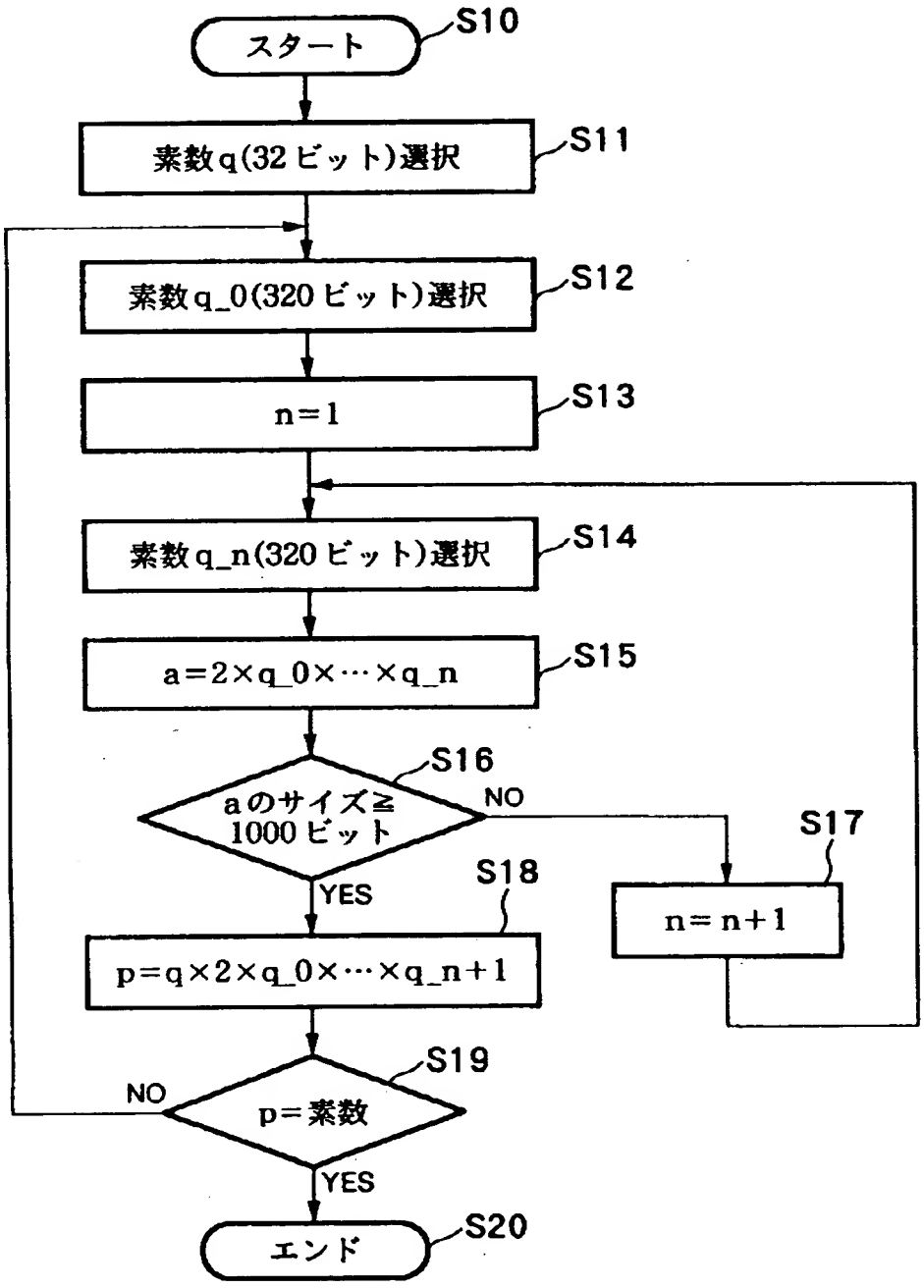


出証特２０００－３０６２４５９

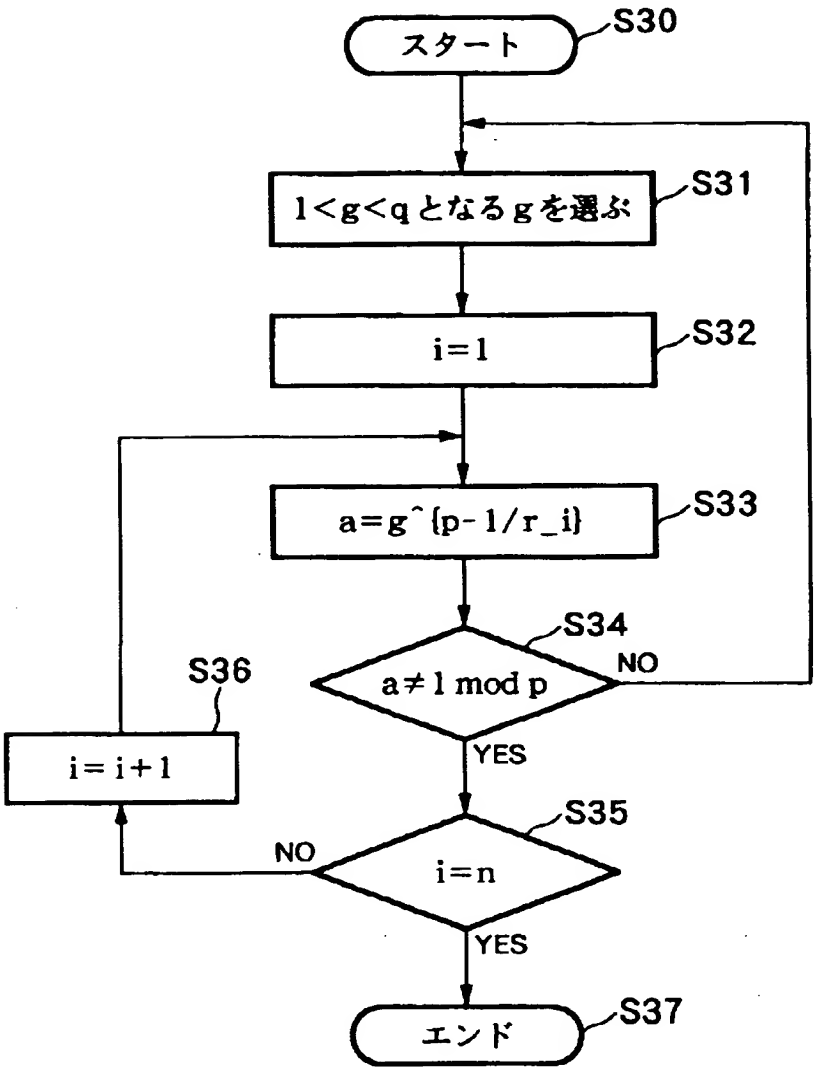
【図３】


31
素数p,q
法pに関する原始根g
32
$h = g^{\frac{p-1}{q}} \bmod p$
33
秘密鍵CK
34
公開鍵UK
$UK = h^{p-1-CK} \bmod p$
35
商品番号PN
36
ドングルID番号DID
プロダクトID番号PID
37
ハッシュ函数H
販売会社
素数p,q
(ソフトウエア)
$h = g^{\frac{p-1}{q}} \bmod p$
(ソフトウエア)
公開鍵UK
商品番号PN
(ソフトウエア)
ドングルID番号DID
プロダクトID番号PID
ドングル、ICカード
ハッシュ函数H
(ソフトウエア)
利用者

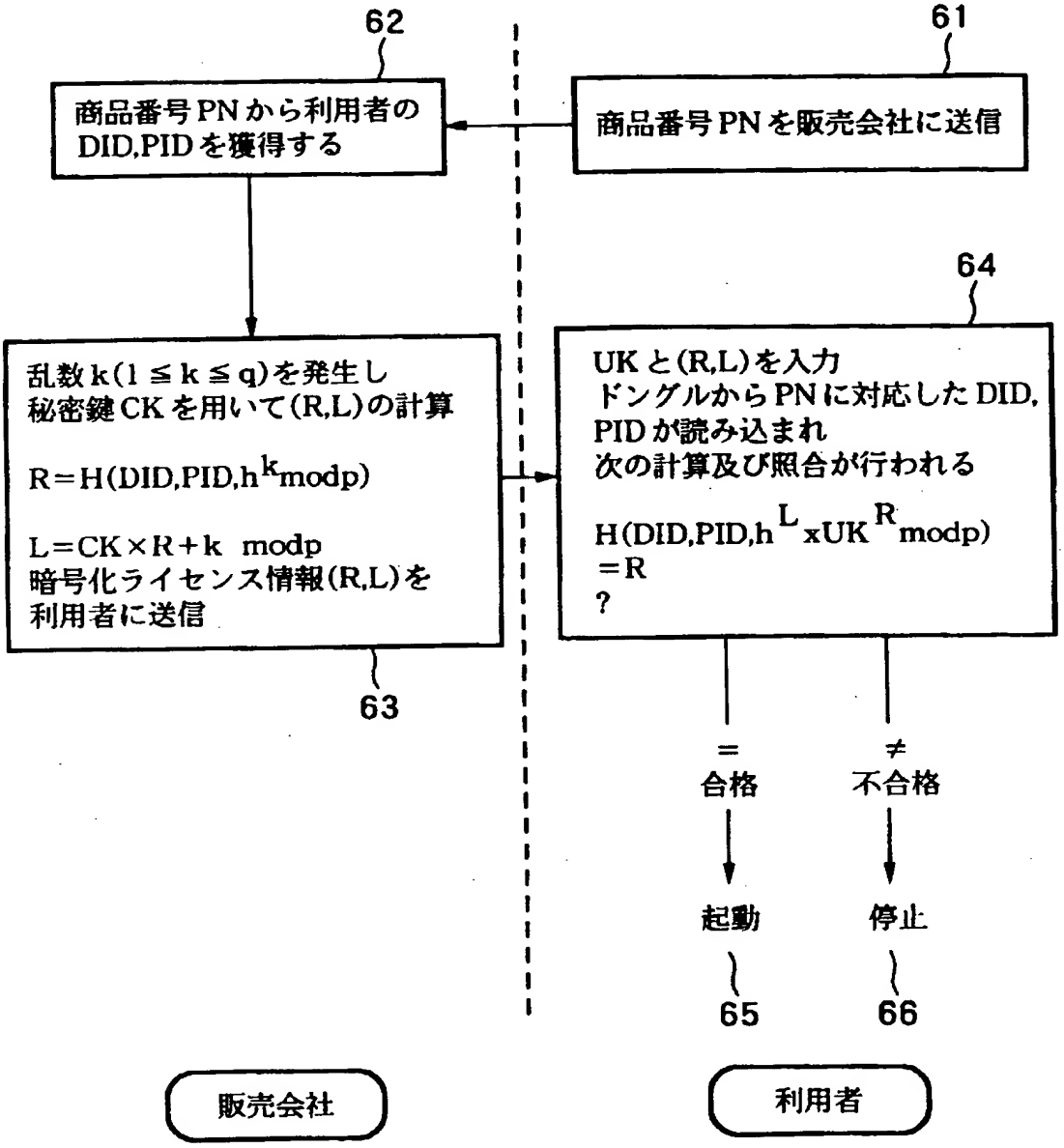
【図４】


スタート
S10
素数q(32ビット)選択
S11
素数q_0(320ビット)選択
S12
n=1
S13
素数q_n(320ビット)選択
S14
a=2×q_0×…×q_n
S15
aのサイズ≧
1000ビット
S16
NO
S17
n=n+1
YES
S18
p=q×2×q_0×…×q_n+1
S19
NO
p=素数
YES
エンド
S20

【図５】


スタート
S30
1<g<qとなるgを選ぶ
S31
i=1
S32
a=g^{p-1/r_i}
S33
S34
a≠1 mod p
NO
YES
S36
i=i+1
S35
i=n
NO
YES
エンド
S37

【図６】


62
61
商品番号PNから利用者のDID,PIDを獲得する
商品番号PNを販売会社に送信
64
乱数k(1≦k≦q)を発生し
秘密鍵CKを用いて(R,L)の計算
R=H(DID,PID,h^k modp)
L=CK×R+k modp
暗号化ライセンス情報(R,L)を利用者に送信
63
UKと(R,L)を入力
ドングルからPNに対応したDID,PIDが読み込まれ
次の計算及び照合が行われる
H(DID,PID,h^L xUK^R modp)
=R
?
=
合格
≠
不合格
起動
停止
65
66
販売会社
利用者

【書類名】　　要約書

【要約】

【課題】所望の形態でソフトウエアの使用を制御することができ、バージョンアップにも容易に対応できるようなソフトウエア使用制御方法を提供する。

【解決手段】販売会社は、ソフトウエアにパスワードを添付し、ドングルに識別情報を内包させ、利用者に配付する。また、秘密鍵と公開鍵を作成し、利用者に公開鍵を伝達する。利用者がライセンスを得ようとした場合、パスワードを販売会社に送信する。販売会社は、パスワードに基づいて識別情報を検出し、秘密鍵を用いて暗号化し、暗号化ライセンス情報として利用者に送信する。利用者は、暗号化ライセンス情報を公開鍵により復号し、ドングルに内包してある識別情報と照合する。照合に合格すれば、ソフトウエアは有効に起動され、失敗すればソフトウエアの実行を停止する。

【選択図】　　図１

出証特２０００－３０６２４５９

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社